Securing a Debian Laptop Against Physical Attacks

A practical guide for full-disk encryption, secure suspend, hibernation, and operational hardening on Debian Unstable

Updated: 06 August 2026

1. Why This Matters

Full-disk encryption (LUKS) only fully protects your data when the machine is powered off. While the laptop is suspended (sleep mode), the encryption keys normally remain in RAM. An attacker who obtains the powered laptop (theft or seizure) can potentially extract those keys via cold-boot attacks or direct memory access. This guide configures the system so that closing the lid wipes the encryption keys from memory and forces a passphrase prompt on resume.

Target setup: Lenovo laptop · Debian Unstable · LUKS full-disk encryption · GNOME desktop.

2. Current Working Configuration (Recommended)

After testing, the following combination gives the best practical security while remaining usable:

Component	Setting
Lid close action	suspend (pure suspend, not suspend-then-hibernate)
Key wiping on suspend	cryptsetup-suspend package (installed & active)
Automatic hibernate later	Optional via HibernateDelaySec (currently disabled for reliability)
Hibernation support	Working — resume= parameter added to GRUB
Swap	/dev/mapper/vg-swap_1 (encrypted, 24 GiB)
GNOME Hibernate button	Enabled via polkit rule + extension

Why pure suspend on lid close? The hybrid “suspend-then-hibernate” path was skipping the cryptsetup-suspend key-wipe step. Pure suspend reliably triggers key removal. You still get fast resume and the machine can be configured to hibernate later if desired.

3. Essential Packages & Configuration Files

3.1 Install cryptsetup-suspend

This package automatically runs `cryptsetup luksSuspend` before the system enters suspend, removing the LUKS master keys from RAM. On resume you must re-enter the passphrase.

```
sudo apt update && sudo apt install cryptsetup-suspend
```

3.2 Lid close behaviour

File: `/etc/systemd/logind.conf.d/lid.conf`

```
[Login]
```

```
HandleLidSwitch=suspend
HandleLidSwitchExternalPower=suspend
HandleLidSwitchDocked=suspend
```

After editing, apply with: `sudo systemctl restart systemd-logind` (you will be logged out).

3.3 Hibernation resume parameter (GRUB)

For reliable hibernation the kernel must know the resume device. Edit `/etc/default/grub`:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet resume=/dev/mapper/vg-swap_1"
```

Then run: `sudo update-grub && sudo update-initramfs -u -k all`

Also make sure the file `/etc/initramfs-tools/conf.d/resume` exists and contains the correct device:

```
RESUME=/dev/mapper/vg-swap_1
```

3.4 Enable Hibernate in GNOME power menu

Create the polkit rule `/etc/polkit-1/rules.d/10-enable-hibernate.rules`:

```
polkit.addRule(function(action, subject) {
    if (action.id == "org.freedesktop.login1.hibernate" ||
        action.id == "org.freedesktop.login1.hibernate-multiple-sessions" ||
        action.id == "org.freedesktop.upower.hibernate" ||
        action.id == "org.freedesktop.login1.handle-hibernate-key" ||
        action.id == "org.freedesktop.login1.hibernate-ignore-inhibit")
    {
        return polkit.Result.YES;
    }
});
```

Install an extension that adds the button (e.g. `gnome-shell-extension-hibernate-status` or the “Power Off Options” extension from extensions.gnome.org). Log out / restart GNOME Shell afterwards.

4. How to Verify Everything Works

Test 1 — Key wipe on suspend

1. Run `systemctl suspend` or close the lid.
2. Wait a few seconds, then open the lid / wake the machine.
3. You **must** be prompted for the LUKS passphrase. If the session resumes without a prompt, the keys were not wiped.

Test 2 — Hibernation

1. Run `systemctl hibernate` (or use the GNOME Hibernate button).
2. The machine should power off completely.
3. Press the power button later — it should resume the previous session after the LUKS passphrase.

If resume fails after a forced reboot, the hibernation image may be invalid. A normal boot will occur. This is expected and safer than loading a corrupted image.

5. Additional Hardening Recommendations

5.1 Firmware / BIOS

• Set a strong BIOS/UEFI supervisor password.
• Enable Secure Boot.
• Disable booting from external media if you do not need it.
• Consider an ATA hard-disk password if the firmware offers it.

5.2 Operational habits

• Fully power off the laptop when the risk of physical access is high (travel, overnight, etc.). Suspend is convenient; power-off is stronger.
• Use a long, high-entropy LUKS passphrase (diceware 6+ words is excellent).
• Keep a short screen-lock timeout (30–60 seconds).
• Never leave the machine unlocked and unattended.
• Prefer a separate USB keyfile for one LUKS keyslot that you carry with you (passphrase remains the backup).

5.3 Software hygiene

• Stay updated (you are on Unstable — good for timely security fixes).
• Consider USBGuard to restrict unauthorized USB devices.
• Maintain offline encrypted backups (borgbackup or restic recommended).
• For very high-threat work, compartmentalize with separate user accounts or even Qubes-style isolation.

6. Important Limitations

• **cryptsetup-suspend only protects the LUKS keys.** Other sensitive data still present in RAM (SSH keys, open documents, browser sessions, etc.) can theoretically be recovered until the machine fully powers off or hibernates.
• Cold-boot attacks remain possible for a short window after power loss, especially if the RAM is cooled.
• Sophisticated attackers with specialized hardware can still attempt advanced memory extraction. No consumer configuration is perfect against a well-resourced adversary who obtains the live machine.
• Always prefer full power-off when the threat level rises.

7. Quick Command Reference

Action	Command
Suspend (wipe keys)	`systemctl suspend`
Hibernate	`systemctl hibernate`
Check cryptsetup-suspend	`dpkg -l | grep cryptsetup-suspend`
Check resume device	`cat /etc/initramfs-tools/conf.d/resume`
Check kernel resume param	`cat /proc/cmdline | tr ' ' '\n' | grep resume`
Restart logind after lid change	`sudo systemctl restart systemd-logind`
Update GRUB + initramfs	`sudo update-grub && sudo update-initramfs -u -k all`

Note: This configuration significantly raises the bar against casual and many professional physical attacks while keeping daily use convenient. It is not absolute security — nothing is — but it is one of the stronger practical setups available on a normal Linux laptop. Re-test the suspend passphrase prompt after any major system update.

August 2026